Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Friday, March 31, 2006

Off-the-record conversations for the Internet

There are many great ideas that have been worked on in the cryptographic theory community that I've long wanted to see implemented in practical tools. Two of these, mathematically deniable authentication and forward secrecy, have now been implemented along with encryption by Ian Goldberg and Nikita Borisov to create the off-the-record messaging software OTR. Now you can have a conversation on the Internet as if it was just you and your buddy on a golf course. You do have to trust that your buddy on the golf course is not wearing a wire, and here Alice has to trust that Bob is not recording the conversation and vice versa.

With mathematical deniability, even if your chat buddy records the conversation, third parties cannot mathematically prove that it was you doing the chatting. This is of limited practicality for legal purposes unless you use OTR via an onion router or similar: otherwise there is enough associated log data to prove Bob's identity in court even if mathematically it could be forged. Even an onion router won't save you if you leave identifying information in the actual conversation and your chat buddy records the conversation. This is because the laws of evidence typically put the burden of proving that such recorded data was forged on the person it is being used against. Nevertheless, in the normal course of operations presumably OTR lives up to its name and does not record the conversation, and your chat buddy would have to go way out of his way to make it do so.

Of more practical use is the forward secrecy, which means that if your chat today is recorded by a third party in the encrypted form over which it is sent across the Internet, and that third party discovers your chat key in the future, that key can't be used to compromise the recorded but encrypted message. "Forward secrecy" means the key you used was destroyed after use, (like on Mission Impossible but automatically instead of with the self-destruct sequence drama), and even if future key(s) are compromised they can't be used to reconstruct the current key, and thus can't be used to decipher the current chat session.

This presentation gives a good overview of the messaging software's rationale and the basics of how mathematically deniable authentication and forward secrecy work. It points out that the law endorses off-the-record phone conversations: normally and in most jurisdictions recording phone conversations without consent is illegal. Cryptography, for the limited problems it actually solves, is far more secure than the law.

Posted by Nick Szabo at 9:14 PM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ▼ March (11)
    - Off-the-record conversations for the Internet
    - Shared key generation using quasars
    - Corporate origins of the United States
    - Metabolite prediction
    - Estimating inflation
    - Rawlsians' maximin: preposterous risk aversion
    - The Magna Carta, Pt. I
    - Property in everything: some background to the Mag...
    - BlackBerry settlement
    - Why are wages flat and

inequality growing?

Quantum dot control over light and heat

► February (10)

► January (26)

► 2005 (44)

Simple theme. Powered by Blogger.